(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 November 2002 (28.11.2002)

PCT

(10) International Publication Number
WO 02/096028 A1

(51) International Patent Classification[7]: H04L 12/22, G06F 11/00, H04L 9/00

(21) International Application Number: PCT/KR02/00891

(22) International Filing Date: 14 May 2002 (14.05.2002)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
2001/28052 22 May 2001 (22.05.2001) KR

(71) Applicant *(for all designated States except US)*: **INZEN CO., LTD.** [KR/KR]; 4/5F Mirae Asset B/D, 996-17 Daechi-Dong, Kangnam-Gu, Seoul 135-280 (KR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HAN, Dong-Hun** [KR/KR]; 516-1102 Ahreum Maeul Apt., 140 Imae-Dong, Bundang-Gu, Sungnam-Si, Kyunggi-Do 463-736 (KR).

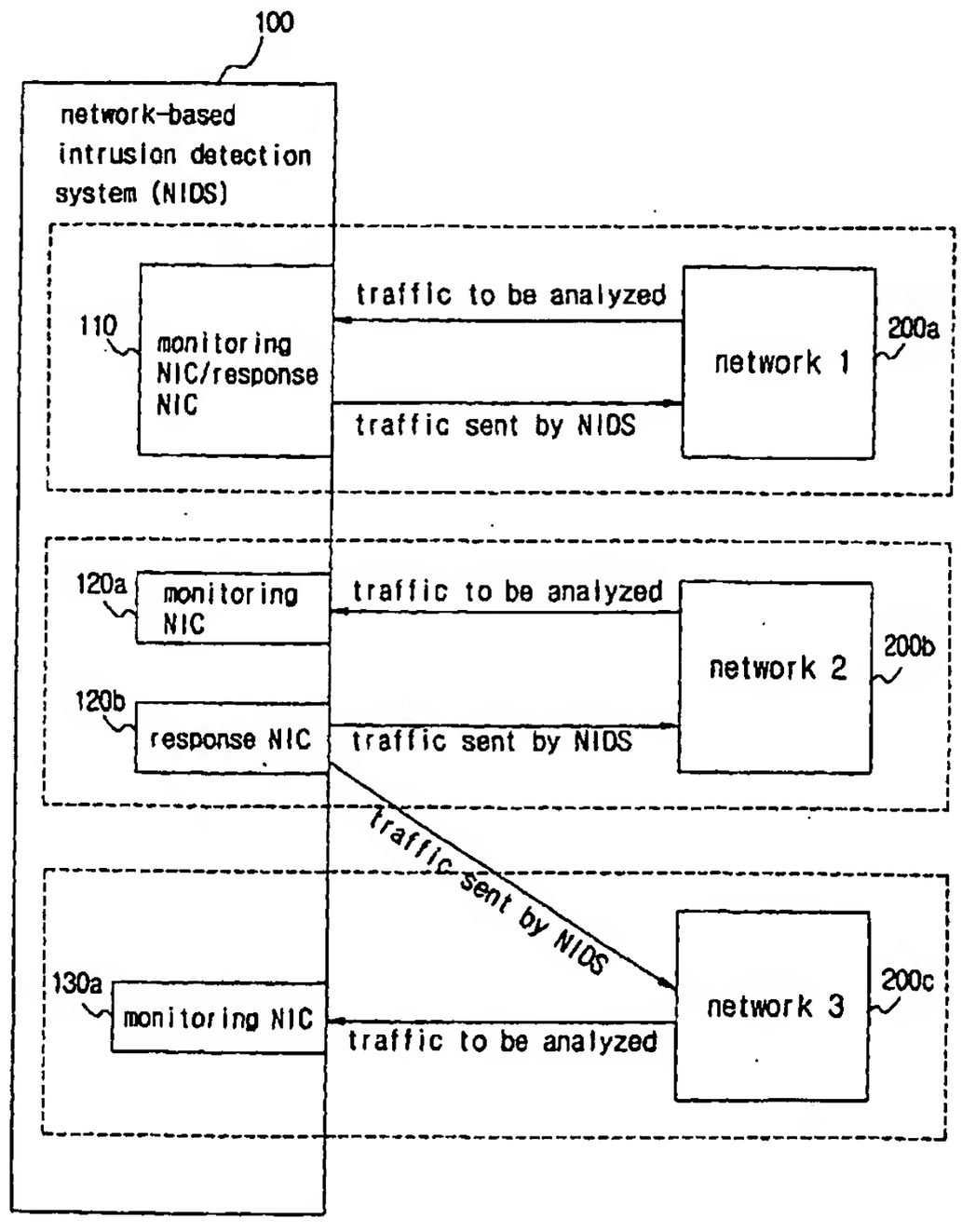
(74) Agent: **L & K PATENT FIRM**; 701, Daekun Bldg., 822-5 Yeoksam-Dong, Kangnam-Gu, Seoul 135-080 (KR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: NETWORK BASED INTRUSION DETECTION SYSTEM



(57) Abstract: A network-based intrusion detection system comprising at least one monitoring network interface card (NIC) for collecting packets of traffic to be analyzed from a network, and at least one response NIC for sending a packet for execution of a suspicious network activity operation and session kill operation to the network Where a plurality of monitoring NICs analyze traffic, they possess response NICs in an individual or shared manner, respectively. A response gateway is further provided to route a packet from a response NIC to the network under the condition that the response NIC cannot send the packet directly. Therefore, the network-based intrusion detection system can actively interrupt and hinder intrusion attempts irrespective of a network configuration type upon detecting network intrusions such as hacking, service attacks, scanning, etc., thereby minimizing improper measures to hacking and accurately monitoring a plurality of networks at the same time.

WO 02/096028 A1

Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*

NETWORK BASED INTRUSION DETECTION SYSTEM

Technical Field

The present invention relates to a network-based intrusion detection system (NIDS), and more particularly to a network interface card configuration of an NIDS which analyzes all traffic flowing through a network, detects dangerous or potentially dangerous activities as a result of the analysis and interrupts the detected activities.

Background Art

A network-based intrusion detection system (NIDS) generally functions to analyze all traffic flowing through a network, detect dangerous or potentially dangerous activities as a result of the analysis, interrupt the detected activities and inform a manager of the activity interruption.

Such activity interruption may be roughly classified into two operations. One is called a suspicious network activity (SNA) operation, which hinders "low level scanning/attack" using fundamental vulnerabilities of a transmission control protocol/Internet protocol (TCP/IP), such as a vulnerability analysis, network service search,

operating system type determination, denial of service (DoS) attack, etc., and the other is called a session kill operation, which forcibly disconnects a TCP connection attempting a dangerous activity.

Both these two operations are performed by sending network packets with specific functions to corresponding networks or hosts.

In this regard, both the SNA operation and session kill operation can be conducted under the condition that the NIDS is able to send a packet to a corresponding network or host.

Fig. 1 is a block diagram showing the construction of a conventional network-based intrusion detection system employing an L2 switch supported with only a forwarding function.

The conventional network-based intrusion detection system (NIDS) is adapted to receive a packet from a network through a network interface card (NIC), analyze the contents of the received packet and send a packet to the network to forcibly terminate a specific session if necessary.

A plurality of NICs may be provided in the NIDS although one NIC is shown in Fig. 1 to be provided in the NIDS.

On the other hand, the suspicious network activity (SNA) operation and session kill operation cannot be performed if the NIC cannot send any packet to the network

due to limitations of equipment in the network.

For example, a packet cannot be sent to the network if the network equipment has a port connected to a packet collection NIC (monitoring NIC) in the NIDS for transferring a packet in a forwarding manner, not in a mirroring manner.

In other words, in the case where the NIDS performs packet sending and receiving operations through the same NIC, it sends a packet from the NIC to a forwarding port on the network. In this case, the sent packet does not actually arrive at the network, thereby making it impossible to actively prevent hacking.

Disclosure of the Invention

Therefore, the present invention has been made in view of the above problems, and it is an object of the present invention to provide a network-based intrusion detection system (NIDS) which is capable of overcoming limitations of network associated hardware by actively interrupting and hindering intrusion attempts, irrespective of a network configuration type, upon detecting network intrusions such as hacking, service attacks, scanning, etc.

It is another object of the present invention to provide a network-based intrusion detection system (NIDS) which has a plurality of packet collection network interface

cards (NICs), each of which possesses a proper response NIC and is secured in its operation.

In accordance with the present invention, the above and other objects can be accomplished by the provision of a network-based intrusion detection system for analyzing all traffic flowing through a network, detecting dangerous or potentially dangerous activities as a result of the analysis and performing a suspicious network activity operation and a session kill operation with respect to the detected activities to interrupt and prevent hacking, the network-based intrusion detection system comprising at least one first-type network interface card module, the first-type network interface card module including: a monitoring network interface card for collecting packets of traffic to be analyzed from the network; and a response network interface card for sending a packet for execution of the suspicious network activity operation and session kill operation to the network.

Preferably, the network-based intrusion detection system may further comprise at least one second-type network interface card module, the second-type network interface card module including only one monitoring network interface card for collecting packets of traffic to be analyzed from the network.

More preferably, the second-type network interface

card module may share the response network interface card of the first-type network interface card module with the first-type network interface card module, the response network interface card including network response environment information of the second-type network interface card module in order to send to the network response packets to the packets collected by the monitoring network interface card of the second-type network interface card module.

Preferably, the network-based intrusion detection system may further comprise a response gateway for routing the packets for execution of the suspicious network activity operation and session kill operation from the response network interface card to the network.

Preferably, the monitoring network interface card and response network interface card of the first-type network interface card module may be configured to be integral with each other.

Alternatively, the monitoring network interface card and response network interface card of the first-type network interface card module may be configured separately from each other.

Brief Description of the Drawings

The above and other objects, features and other

advantages of the present invention will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings, in which:

Fig. 1 is a block diagram showing the construction of a conventional network-based intrusion detection system employing an L2 switch supported with only a forwarding function;

Fig. 2 is a block diagram showing a preferred embodiment of a network-based intrusion detection system in accordance with the present invention;

Fig. 3 is a block diagram showing an alternative embodiment of the network-based intrusion detection system in accordance with the present invention; and

Fig. 4 is a schematic view of a setup program of the network-based intrusion detection system in accordance with the present invention.

Best Mode for Carrying Out the Invention

Fig. 2 is a block diagram showing a preferred embodiment of a network-based intrusion detection system (NIDS) in accordance with the present invention, which is denoted by the reference numeral 100.

As shown in this drawing, the NIDS 100 comprises three intrusion detection modules.

Hereinafter, a network interface card for collecting packets of traffic to be analyzed from a network will be referred to as a monitoring NIC, and a network interface card for sending a packet for execution of a suspicious network activity (SNA) operation and session kill operation to the network will be referred to as a response NIC (RN).

The first module is a network interface card module 110 including a monitoring NIC and a response NIC which is integral with the monitoring NIC. The monitoring NIC is adapted to collect packets of traffic to be analyzed from a network 1 200a, and the response NIC is adapted to send a packet for execution of the SNA operation and session kill operation to the network 1 200a. With this construction, the network interface card module 110 performs both the operations of the monitoring NIC and response NIC.

That is, the network interface card module 110 collects packets of traffic to be analyzed from the network 1 200a via the same network interface card, and sends a packet for execution of the SNA operation and session kill operation to the network 1 200a via the same network interface card.

The second module is a network interface card module including a monitoring NIC 120a and a response NIC 120b, individually. The monitoring NIC 120a is adapted to collect packets of traffic to be analyzed from a network 2 200b, and

the response NIC 120b is adapted to send a packet for execution of the SNA operation and session kill operation to the network 2 200b.

That is, the second module collects packets of traffic to be analyzed from the network 2 200b via the monitoring NIC 120a, and sends a packet for execution of the SNA operation and session kill operation to the network 2 200b via the response NIC 120b which is configured separately from the monitoring NIC 120a.

The third module is a network interface card module including only one monitoring NIC 130a for collecting packets of traffic to be analyzed from a network 3 200c. This third module shares the response NIC 120b with the second module to send a packet for execution of the SNA operation and session kill operation to the network 3 200c.

In other words, the third module collects packets of traffic to be analyzed from the network 3 200c via the monitoring NIC 130a, and sends a packet for execution of the SNA operation and session kill operation to the network 3 200c via the response NIC 120b of the second module.

Notably, the shared response NIC 120b must have information about a response scheme of the monitoring NIC 130a in order to send a packet in a proper manner.

Fig. 3 is a block diagram showing an alternative embodiment of the network-based intrusion detection system in

accordance with the present invention.

In this embodiment, the network-based intrusion detection system 100 further comprises a response gateway 300 for routing a response packet.

The network-based intrusion detection system 100 routes and sends a packet for execution of the SNA operation and session kill operation from a response NIC therein to a network through the response gateway 300. As a result, even though the response NIC cannot be connected to a middle-stage network or the network is experiencing problems, the response operation can be performed according to the router's ability.

On the other hand, the network-based intrusion detection system 100 pairs a monitoring NIC and a response NIC and determines a packet sending mode, with respect to each of the above modules, and collects information necessary for packet sending in the determined mode, for example, destination media access control (MAC) addresses which are hardware addresses of devices connected to a shared medium of a packet destination.

The network-based intrusion detection system 100 then determines from settings one of the response NICs through which a packet will be sent, and sends the packet to a MAC address of a corresponding destination through the determined response NIC.

In order for a packet to arrive at a specific host in an Ethernet environment, the network-based intrusion detection system must recognize a destination MAC address.

This MAC address may be a MAC address of a gateway for sending a packet to a different network, or a MAC address of a host connected to a subnet of the same Ethernet.

Similarly, a response NIC may designate a MAC address of a specific host corresponding to an IP address, or a self-MAC address of the response NIC as a source MAC address of a packet to be sent.

The above procedures must be manually performed with reference to a network configuration because they are based on a network connection state.

MAC addresses may be roughly classified into two types, a source MAC address and a destination MAC address. The source MAC address is a MAC address of a packet sending NIC, and the destination MAC address is a MAC address of a packet receiving NIC.

An RN may selectively use three types of source MAC addresses when sending a packet. The first type is an original MAC address. In this case, the RN is connected to, for example, a dummy hub. The dummy hub is not influenced by any MAC address at all, so a MAC address corresponding to an IP address may be used. In this regard, it is most preferable to use an original MAC address to produce no side effect.

The second type is a self-MAC address of the RN. In this case, the RN is connected to, for example, an L2 switch. Because the L2 switch performs a switching operation in response to a MAC address, a problem may occur when a MAC address of a different computer is used. On the other hand, the self-MAC address of the RN may be unable to be used where a MAC address variation detection host, intrusion detection system (IDS) or firewall is provided. In this case, however, the self-MAC address of the RN can be used by removing the MAC address variation detection function from a corresponding NIDS or firewall.

The third type is a specific MAC address, which is used for a specific purpose or as needed. In this case, there must be designated a MAC address which is to be used.

Likewise, the RN may selectively use three types of destination MAC addresses when sending a packet. The first type is an original MAC address. In this case, the RN is connected to a dummy hub. The dummy hub is not influenced by any MAC address at all, so a MAC address corresponding to an IP address may be used. In this regard, it is most preferable to use an original MAC address to produce no side effect.

The second type is a MAC address of a response gateway. For setup of the response gateway, it is necessary to process address resolution protocol (ARP) information to perform a mapping operation for conversion of an IP address into an

Ethernet address. A MAC address of the response gateway, obtained as a result of the processing, is used as a destination MAC address to send a packet.

The third type is a specific MAC address, which is used for a specific purpose or as needed. In this case, there must be designated a MAC address which is to be used.

In the present invention, in the case where a plurality of monitoring NICs analyze traffic, they possess response NICs, respectively. In this case, one response NIC may be set with respect to several monitoring NICs. In this connection, each response NIC must have setting information for determination of response MAC addresses with respect to one or more monitoring NICs.

A response processing module has a mode for selection of MAC addresses with respect to all monitoring NICs associated therewith. Upon receiving a response request, the response processing module determines a MAC address to be used for a corresponding response. This MAC address determination can be made by transferring to a corresponding response NIC information regarding a monitoring NIC through which traffic is received, along with the traffic.

Fig. 4 is a schematic view of a setup program of the network-based intrusion detection system in accordance with the present invention.

When module (n) managers are initialized, they read

their respective settings from a setting file or registry, initialize NIC (n) instances to be used, with the read settings, and store desired information according to the read settings. If a specific one of the module (n) managers requests a corresponding one of the NIC (n) instances to send a packet on the basis of the stored information, the corresponding NIC (n) instance determines a hardware address to be used for the packet sending and performs a response to the request on the basis of the determined hardware address.

Therefore, according to the present invention, it is possible to minimize improper measures to hacking, resulting from limitations of network equipment, and to accurately monitor a plurality of networks at the same time.

Industrial Applicability

As apparent from the above description, the present invention provides a network-based intrusion detection system which is capable of overcoming limitations of network associated hardware by actively interrupting and hindering intrusion attempts, irrespective of a network configuration type, upon detecting network intrusions such as hacking, service attacks, scanning, etc. Therefore, the present network-based intrusion detection system can minimize improper measures to hacking and accurately monitor a plurality of

networks at the same time.

Although the preferred embodiments of the present invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that various modifications, additions and substitutions are possible, without departing from the scope and spirit of the invention as disclosed in the accompanying claims.

Claims:

1. A network-based intrusion detection system for analyzing all traffic flowing through a network, detecting dangerous or potentially dangerous activities as a result of the analysis and performing a suspicious network activity operation and a session kill operation with respect to the detected activities to interrupt and prevent hacking, said network-based intrusion detection system comprising at least one first-type network interface card module, said first-type network interface card module including:

a monitoring network interface card for collecting packets of traffic to be analyzed from said network; and

a response network interface card for sending a packet for execution of said suspicious network activity operation and session kill operation to said network.

2. The network-based intrusion detection system as set forth in claim 1, further comprising at least one second-type network interface card module, said second-type network interface card module including only one monitoring network interface card for collecting packets of traffic to be analyzed from said network.

3. The network-based intrusion detection system as set

forth in claim 2, wherein said second-type network interface card module shares said response network interface card of said first-type network interface card module with said first-type network interface card module, said response network interface card including network response environment information of said second-type network interface card module in order to send to said network response packets to the packets collected by said monitoring network interface card of said second-type network interface card module.

4. The network-based intrusion detection system as set forth in any one of claim 1 to claim 3, further comprising a response gateway for routing the packets for execution of said suspicious network activity operation and session kill operation from said response network interface card to said network.

5. The network-based intrusion detection system as set forth in any one of claim 1 to claim 3, wherein said monitoring network interface card and response network interface card of said first-type network interface card module are configured to be integral with each other.

6. The network-based intrusion detection system as set

forth in any one of claim 1 to claim 3, wherein said monitoring network interface card and response network interface card of said first-type network interface card module are configured separately from each other.

FIG 1

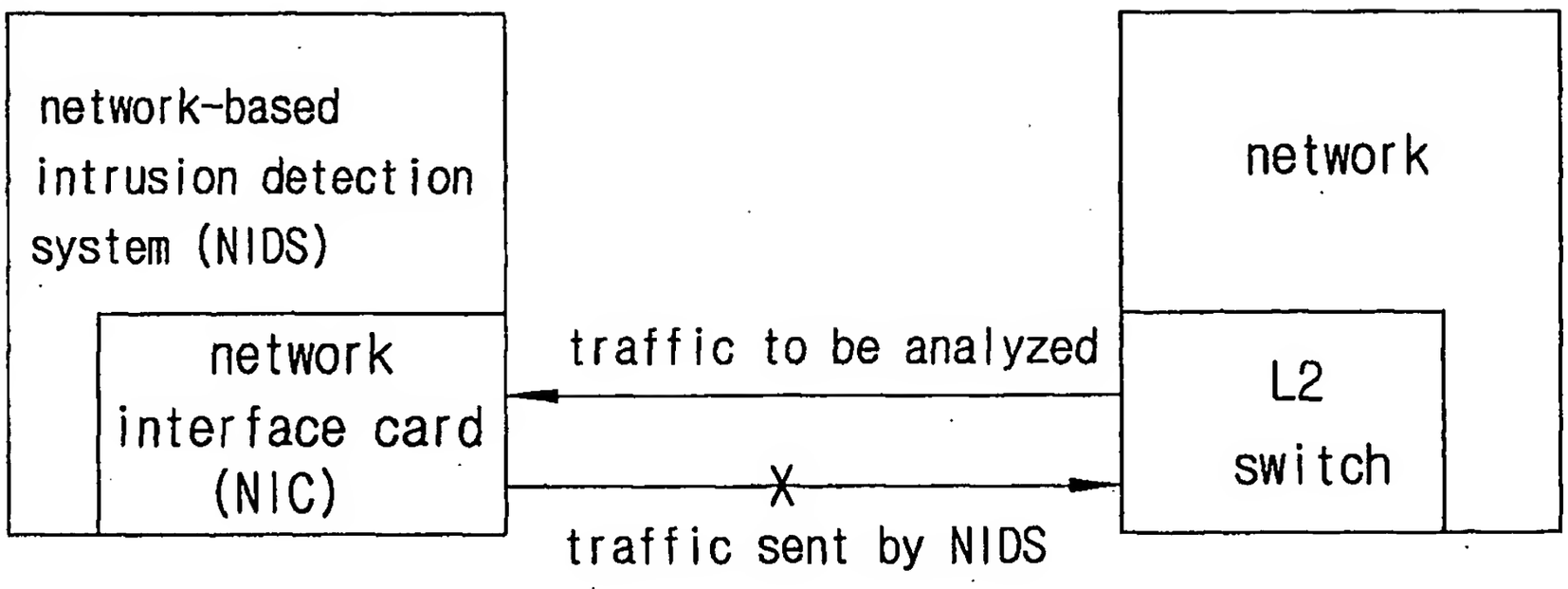

network-based
intrusion detection
system (NIDS)
network
interface card
(NIC)
traffic to be analyzed
X
traffic sent by NIDS
L2
switch
network

FIG 2

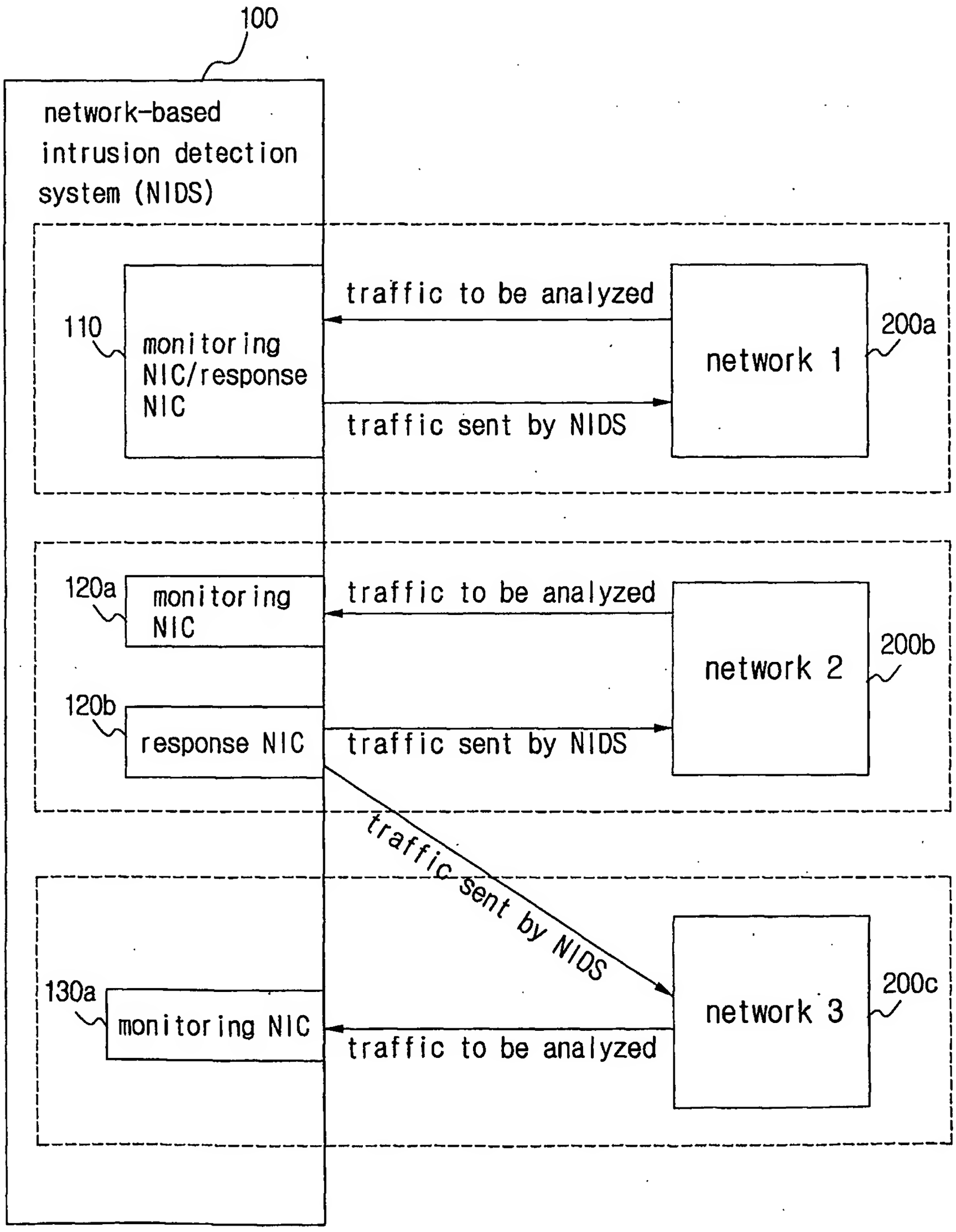

100
network-based intrusion detection system (NIDS)
110
monitoring NIC/response NIC
traffic to be analyzed
traffic sent by NIDS
200a
network 1
120a
monitoring NIC
120b
response NIC
traffic to be analyzed
traffic sent by NIDS
200b
network 2
traffic sent by NIDS
130a
monitoring NIC
traffic to be analyzed
200c
network 3

FIG 3

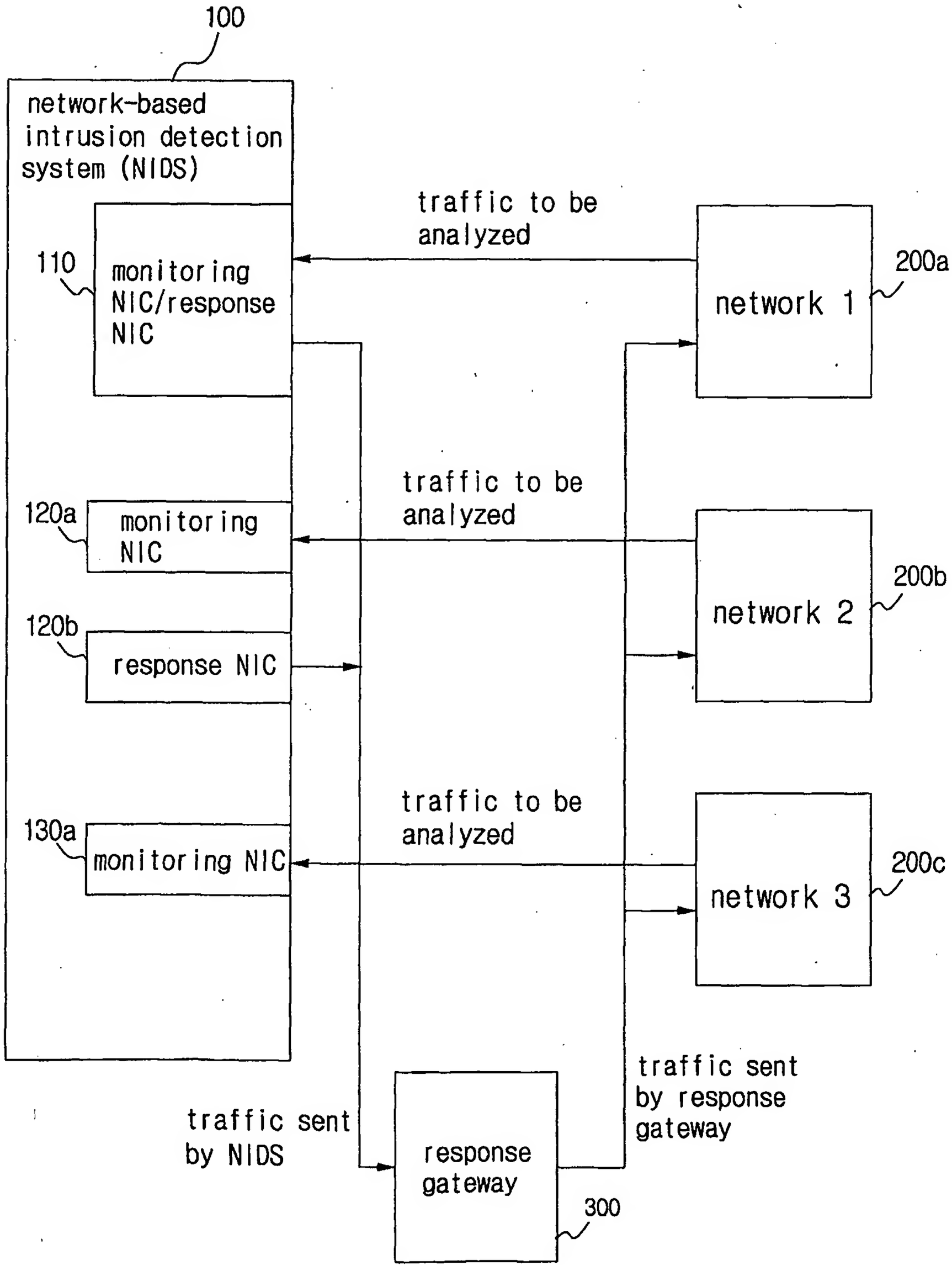
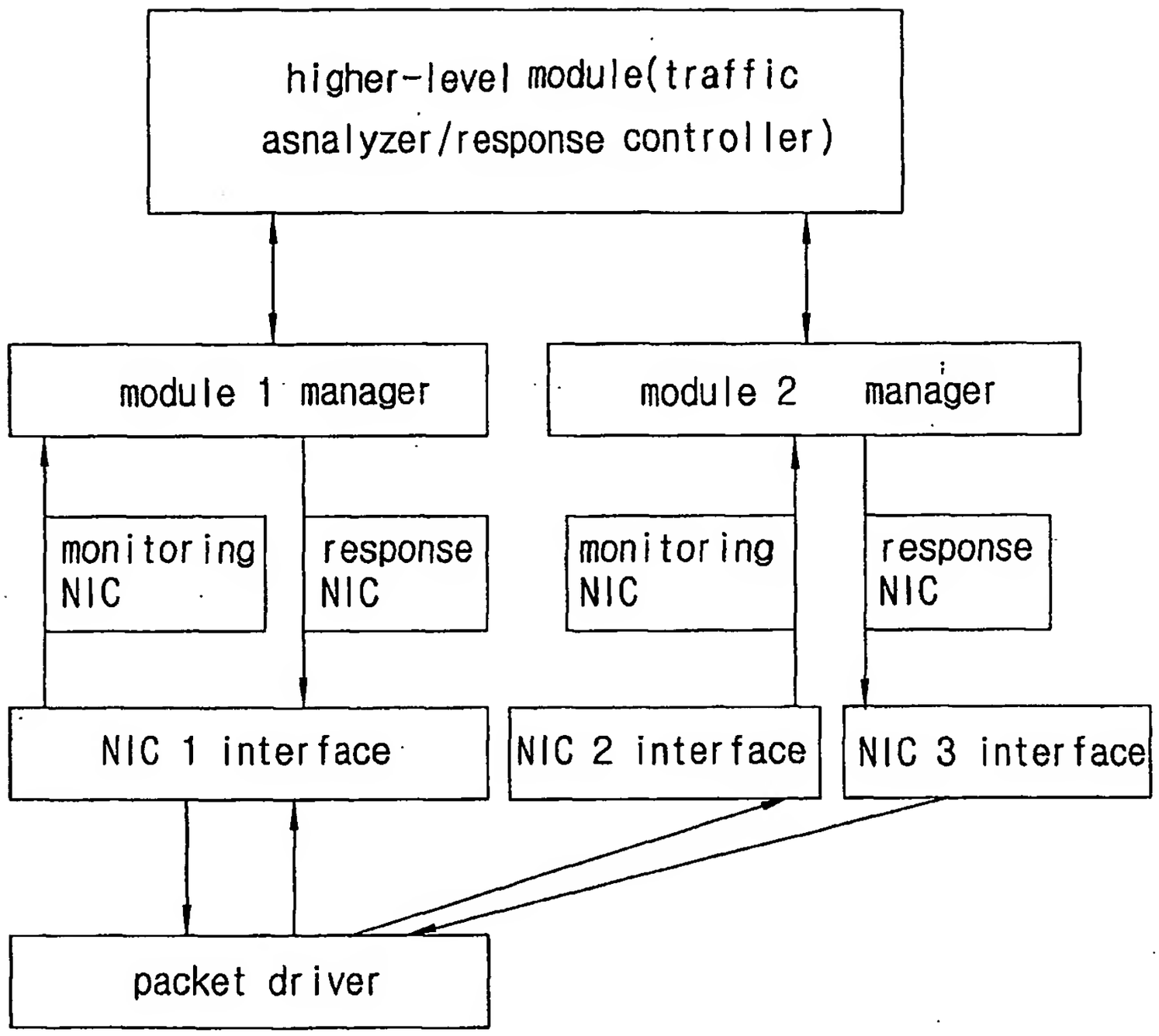

100
network-based intrusion detection system (NIDS)
110
monitoring NIC/response NIC
traffic to be analyzed
200a
network 1
120a
monitoring NIC
traffic to be analyzed
200b
network 2
120b
response NIC
130a
monitoring NIC
traffic to be analyzed
200c
network 3
traffic sent by response gateway
traffic sent by NIDS
response gateway
300

FIG 4


higher-level module(traffic asnalyzer/response controller)
module 1 manager
module 2 manager
monitoring NIC
response NIC
monitoring NIC
response NIC
NIC 1 interface
NIC 2 interface
NIC 3 interface
packet driver

INTERNATIONAL SEARCH REPORT

mational application No.
PCT/KR02/00891

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L 12/22 G06F 11/00 H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7 H04L 12/22 G06F 11/00 H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

KOREAN PATENTS AND APPLICATIONS FOR INVENTIONS SINCE 1975
KOREAN UTILITY MODELS AND APPLICATIONS FOR UTILITY MODELS SINCE 1975

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,991,881 A (HARRIS CORP.) 23 NOVEMBER 1999	1 - 6
A	US 5,414,833 A (IBM) 9 MAY 1995	1 - 6
A	EP 985995 A (IBM) 15 MARCH 2000	1 - 6
A	GIOVANNI "NetSTAT: A Network-based Intrusion Detection Approach" In: IEEE Computer Security Applications Conference 1998. Proceedings, 14th Annual, Pages 25-34	1 - 6
A	BISWANATH "Network Intrusion Detection" In: IEEE Network , published May/June 1994, Volume 83, Pages 26-41	1 - 6

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 AUGUST 2002 (27.08.2002)	27 AUGUST 2002 (27.08.2002)

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
HWANG, Eun Taek
Telephone No. 82-42-481-5688

Form PCT/ISA/210 (second sheet) (July 1998)